



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/541,697	04/18/2006	Marian Trinkel	520.1053	1949
7278	7590	04/02/2009		
DARBY & DARBY P.C. P.O. BOX 770 Church Street Station New York, NY 10008-0770			EXAMINER	
			ARCHER, CHRISTOPHER B	
			ART UNIT	PAPER NUMBER
			2432	
			MAIL DATE	DELIVERY MODE
			04/02/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/541,697	Applicant(s) TRINKEL, MARIAN
	Examiner CHRISTOPHER B. ARCHER	Art Unit 2432

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If no period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED. (35 U.S.C. § 133).

Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 12/30/2008.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-20 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-20 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 18 April 2006 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO/OS/02/05)
Paper No(s)/Mail Date 07/07/2008

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____

5) Notice of Informal Patent Application

6) Other: _____

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed January 27, 2009.
2. Claims 1-10 have been amended and claims 11-20 have been added. Pending claims include claims 1-20.
3. Applicant's arguments, see pages 12 and 13 of Applicant's Arguments/Remarks, filed December 20th, 2008, with respect to the newly amended claims have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of the combination of the teachings of Hartman and Fruehauf, necessitated by the amendments.
4. On page 13 of the applicant's remarks, the applicant argues that Hartman combined with Fruehauf does not teach generating at least one key by the central system and a network user simultaneously.
5. The examiner disagrees with the applicant's arguments, as Fruehauf, (column 2, lines 14-34) discloses a system in which the "stored and/or generated encryption keys are preferably time synchronized in the hardware of the authorized user community so that the key used to encrypt data at the sending end is the same key that decrypts the data at the receiving end."

Claim Rejections - 35 USC § 103

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. Claims 1, 2, 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hartman Jr. (5,444,780), hereafter referred to as Hartman, in view of Fruehauf et al. (US 6,590,981), hereafter referred to as Fruehauf.

Regarding claim 1:

Hartman discloses “A method for providing a time stamp by using a tamper-proof time signal via a telecommunications network comprising the steps of:

receiving at a central system a request from a network user for a time signal;

encrypting said time signal by the central system with at least one key;

transmitting the encrypted time signal to the network user via the telecommunications network;

providing the network user with the same at least one key.”

[Hartman column 4, lines 54-56, 66-68; column 5, lines 28-43) discloses a client computer requesting a time signal from a recognized server. The server responds to the request by sending an encrypted time signal to the client. The client then decrypts the time signal using the same key that the server used to encrypt it.]

Hartman fails to explicitly disclose “synchronously generating, at the central system and the network user, the at least one key.”

However, Fruehauf discloses “synchronously generating, at the central system and the network user, the at least one key.”

[(Fruehauf column 2, lines 14-34; column 4, lines 22-64) discloses a system that generates keys synchronously at two different locations.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Hartman to synchronously generate symmetric keys, as taught in Fruehauf, in order to use a symmetric system that changes keys.

Regarding claim 2:

Fruehauf further teaches “The method as recited in claim 1, wherein the synchronously generating is performed so as to change the at least one key changes synchronously after predetermined time intervals.”

[(Fruehauf column 2, lines 7-10, 14-34) discloses a cryptographic communication system with time synchronized keys that change after a predetermined period of time, being used for encryption and decryption between sender and receiver locations.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Hartman to dynamically change symmetric keys, as taught in Fruehauf, as changing keys creates an extremely high entry barrier for hackers, and changing keys synchronously at two different communication points.

Regarding claim 15:

Hartman further teaches “The method as recited in claim 1, further comprising the step of decrypting, by the network user using the at least one key, the transmitted encrypted time signal.”

[(Hartman column 5, lines 38-43) discloses a system where the client decrypts the encrypted time signal that was sent to it from a secure time server.]

Regarding claim 16:

Fruehauf further teaches “The method as recited in claim 1, wherein the central system is a certified central system.”

[(Fruehauf column 3, line 47 to column 4, line 15) discloses a system that uses officially recognized time sources to generate a time signal.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to only use officially recognized time sources, as taught by Fruehauf, in order to prevent potentially erroneous or malicious data from being entered into the secure system.

Regarding claim 17:

Fruehauf further teaches “The method as recited in claim 1, wherein the time signal is an officially recognized time signal.”

[(Fruehauf column 3, line 47 to column 4, line 15) discloses a system that uses officially recognized time sources to generate a time signal.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to only use officially recognized time signals, as taught by Fruehauf, in order to prevent potentially erroneous or malicious data from being entered into the secure system.

8. Claims 3, 9-11, 19, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hartman, in view of Fruehauf, and further in view of Sinha et al. (US 6,944,188), hereafter referred to as Sinha.

Regarding claim 3:

Hartman and Fruehauf disclose: “The method as recited in claim 1,”

[(See rejection for claim 1)]

“so that the respectively assigned at least one respective clock system operate synchronously to generate the at least one key.”

[(Fruehauf column 2, lines 22-34; column 4, lines 22-64) discloses a system that generates keys synchronously at two different locations.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Hartman to synchronously generate symmetric keys, as taught in Fruehauf, in order to prevent the loss or rejection of valid data.

Hartman and Fruehauf fail to explicitly disclose “providing the network user and the central system each with at least one respective clock system.

respectively assigning the at least one respective clock system at the network user to the at least one respective clock system at the central system.”

However, Sinha discloses “providing the network user and the central system each with at least one respective clock system.

respectively assigning the at least one respective clock system at the network user to the at least one respective clock system at the central system.”

[(Sinha column 4, lines 20-23; column 5, lines 51-56, 63-64) discloses a system in which a plurality of clock pairs, in the form of master and slave clocks, are commonly used across a network.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Hartman to allow clocks to be paired in master and slave pairs, as taught by Sinha, so that separate clock pairs may be synchronized by different techniques.

Regarding claim 9:

Hartman discloses “A system for generating a tamper-proof time stamp in network-based communication systems, the system comprising:

“a central system connected to the network-based communication system;
“a network user connected to the network-based communication system; and
“wherein the central system is configured to encrypt a time signal using the at least one changed key, and further configured to send the encrypted time signal to the network user;” and

“wherein the network user is configured to decrypt the encrypted time signal.”

[(Hartman column 4, lines 54-56; column 5, lines 28-43) discloses a system with a server coupled to a client. The server encrypts the time information and sends it to the client for decryption.]

Hartman fails to explicitly disclose “a respective clock system at the network user and at the central system, wherein each of the respective clock systems is assigned to

each other and configured to operate synchronously so as to generate at least one changed key;”

However, Sinha discloses “a respective clock system at the network user and at the central system, wherein each of the respective clock systems is assigned to each other”

[*(Sinha column 4, lines 20-23; column 5, lines 51-56, 63-64) discloses a system containing a plurality of clock pairs, in the form of master and slave clocks, distributed across a network.*]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Hartman to allow clocks to be paired in master and slave pairs, as taught by Sinha, so that separate clock pairs may be synchronized by different techniques.

Sinha fails to explicitly disclose “configured to operate synchronously so as to generate at least one changed key;”

However, Fruehauf discloses “configured to operate synchronously so as to generate at least one changed key;”

[*(Fruehauf column 2, lines 14-34; column 4, lines 22-64) discloses a system that generates keys synchronously at two different locations.*]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Hartman to synchronously generate symmetric keys, as taught in Fruehauf, in order to prevent the loss or rejection of valid data.

Regarding claim 10:

Sinha further discloses “The system as recited in claim 9, wherein the central system includes a time signal transmitter.”

[(Sinha column 3, lines 5-11; column 7, line 61 to column 8, line 3; Fig. 3) discloses a system that uses a transmitter as part of the master clock.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to include a signal transmitter, as taught by Sinha, in order to allow for a communications over a wider area.

Regarding claim 11:

Hartman and Fruehauf disclose: “The method as recited in claim 1,”

[(See rejection for claim 1)]

“so that the assigned at least one respective clock system operate synchronously to change the at least one key.”

[(Fruehauf column 2, lines 14-34; column 4, lines 22-64) discloses a system that generates keys synchronously at two different locations.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Hartman to synchronously generate symmetric keys, as taught in Fruehauf, in order to prevent the loss or rejection of valid data.

Hartman and Fruehauf fail to explicitly disclose “providing the network user and the central system each with at least one respective clock system;

assigning the at least one respective clock system at the network user to the at least one respective clock system at the central system”

However, Sinha discloses “providing the network user and the central system each with at least one respective clock system;

assigning the at least one respective clock system at the network user to the at least one respective clock system at the central system”

[(Sinha column 4, lines 20-23; column 5, lines 51-56, 63-64) discloses a system containing a plurality of clock pairs, in the form of master and slave clocks, distributed across a network.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Hartman to allow clocks to be paired in master and slave pairs, as taught by Sinha, so that separate clock pairs may be synchronized by different techniques.

Regarding claim 19:

Fruehauf further discloses “The method as recited in claim 9, wherein the at least one changed key is synchronously generated at intervals of time.”

[(Fruehauf column 2, lines 7-10, 14-34) discloses a cryptographic communication system with time synchronized keys that change after a predetermined period of time, being used for encryption and decryption between sender and receiver locations.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Hartman to dynamically change symmetric keys, as taught in Fruehauf, as changing keys creates an extremely high entry barrier for hackers, and changing keys synchronously at two different communication points, prevents the loss or rejection of valid data.

Regarding claim 20:

Fruehauf further discloses “The method as recited in claim 9, wherein the time signal is an officially recognized time signal.”

[(Fruehauf column 3, line 47 to column 4, line 15) discloses a system that uses officially recognized time sources to generate a time signal.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to only use officially recognized time sources, as taught by Fruehauf, in order to prevent potentially erroneous or malicious data from being entered into the secure system.

9. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hartman in view of Fruehauf, in view of Crane et al. (US 6,510,236), hereafter referred to as Crane, and further in view of Friedman et al. (US 2002/0019933), hereafter referred to as Friedman.

Regarding claim 4:

Hartman and Fruehauf disclose “The method as recited in claim 1,”

[(See rejection for claim 1)]

“further comprising the steps of: receiving a time signal request, at the central system, from the network user;”

[(Hartman column 4, lines 54-56, 66-68; column 5, lines 28-43) discloses a client computer requesting a time signal from a recognized server.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to only use officially recognized time sources, as taught by Fruehauf, in order to prevent potentially erroneous or malicious data from being entered into the secure system.

Hartman and Fruehauf fail to explicitly disclose “determining, by the central system, a clock system assigned to the network user using a transmitted identifier, wherein the transmitted identifier is the network address of the network user and wherein the at least one key is generated by the assigned clock system.”

However, Crane discloses “determining, by the central system, a clock system assigned to the network user using a transmitted identifier, wherein the transmitted identifier is the network address of the network user.”

[(Crane column 4, line 48 to column 5, line 36) discloses a system in which a device-id is used to locate the corresponding server.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to use a device’s corresponding id, as taught by Crane, as the device’s id is known by both parties and can easily be used to generate corresponding symmetric keys.

Crane fails to explicitly disclose “wherein the at least one key is generated by the assigned clock system.”

However, Friedman discloses “wherein the at least one key is generated by the assigned clock system.”

[Friedman [0106]] discloses a system in which dynamic keys are generated using the present time as a seed.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to use the present time as a seed, as taught by Friedman, as time signals are frequently used in generating pseudo-random numbers.

Regarding claim 18:

Fruehauf further discloses “The method as recited in claim 4, wherein the at least one key is generated using at least one of the assigned clock system and the transmitted identifier.”

[Friedman [0101] discloses a system in which a key is derived using information unique to the particular requesting device.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to use a device’s corresponding id, as taught by Crane, as the device’s id is known by both parties and can easily be used to generate corresponding symmetric keys.

10. Claims 5-8 and 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hartman in view of Fruchauf and further in view of Kara (US 5,982,506), hereafter referred to as Kara.

Regarding claim 5:

Hartman and Fruchauf disclose “A method for transmitting data with a tamper-proof time stamp over a telecommunications network from a first network user to a second network user, comprising the steps of:

obtaining a time signal in accordance with a method as recited in claim 1;”

[(See rejection for claim 1)]

Hartman and Fruchauf fail to explicitly disclose “transmitting the time signal and the data from the first network user to the second network user one of directly and indirectly via the central system.”

However, Kara discloses “transmitting the time signal and the data from the first network user to the second network user one of directly and indirectly via the central system.”

[(Kara column 19, lines 19-31) discloses a system in which a sender and a receiver communicate directly with one another without the intervention of a central system.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Hartman to allow the sender and receiver to communicate with each other without relying on a central system, as taught in Kara, to hasten transaction speed between the two devices.

[(Kara column 4, lines 25-56) discloses an invention that sends a message from a sender to a receiver via a certification system.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Hartman to send a message indirectly through a central system, as taught by Kara, so that the send time may be verified and certified by an external third party.

Regarding claim 6:

Kara further discloses “The method as recited in claim 5, further comprising the steps of:

encrypting, by the first network user, at least one of the data and the time signal during transmission.”

[(Kara column 4, lines 43-48; column 7, lines 43-45) discloses a system in which the electronic document and/or the cipher containing the timestamp may be encrypted.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Hartman to encrypt the electronic document containing the timestamp, as taught by Kara, to prevent potentially erroneous or malicious data from entering into a secure system.

Regarding claim 7:

Kara further discloses “The method as recited in claim 5, wherein the central system is provided at the second network user.”

[(Kara column 25, lines 47-61) discloses a system in which the certification and key distribution authority can be located at the receiving location.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Hartman to allow the central system to be located at the second network user, as taught by Kara, in order to hasten the key generation process and ensure symmetric key coordination.

Regarding claim 8:

Kara further discloses "The method as recited in claim 5, further comprising the step of returning, by the central system, acknowledgement of receipt to the first network user."

[(Kara column 4, line 65 to column 5, line 22) discloses a system in which the receiver sends an acknowledgement message to the certification program which forwards the acknowledgement to the sender upon successful verification.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to forward an acknowledgement message to the sender, as taught by Kara, in order to allow the sender to re-transmit a message if it was not received by the receiver.

Regarding claim 12:

Kara further discloses "The method as recited in claim 6, wherein a central system is provided at the second network user."

[(Kara column 25, lines 47-61) discloses a system in which the certification and key distribution authority can be located at the receiving location.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teachings of Hartman to allow the central system to be located at the second network user, as taught by Kara, in order to hasten the key generation process and ensure symmetric key coordination.

Regarding claim 13:

Kara further discloses "The method as recited in claim 6, wherein the central system is configured to return an acknowledgement of receipt to the first network user."

[(Kara column 4, line 65 to column 5, line 22) discloses a system in which the receiver sends an acknowledgement message to the certification program which forwards the acknowledgement to the sender upon successful verification.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to forward an acknowledgement message to the sender, as taught by Kara, in order to allow the sender to re-transmit a message if it was not received by the receiver.

Regarding claim 14:

Kara further discloses "The method as recited in claim 7, wherein the central system is configured to return an acknowledgement of receipt to the first network user."

[(Kara column 4, line 65 to column 5, line 22) discloses a system in which the receiver sends an acknowledgement message to the certification program which forwards the acknowledgement to the sender upon successful verification.]

It would have been obvious to one of ordinary skill in the art at the time of invention to modify the teaching of Hartman to forward an acknowledgement message to the sender, as taught by Kara, in order to allow the sender to re-transmit a message if it was not received by the receiver.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER B. ARCHER whose telephone number is (571) 270-7308. The examiner can normally be reached on M-F 7:30-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CHRISTOPHER B ARCHER/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432